



REPLY TO  
ATTENTION OF:

**DEPARTMENT OF THE ARMY**  
**HEADQUARTERS, 4TH INFANTRY DIVISION (MECHANIZED) AND FORT CARSON**  
**BLDG 1435, WETZEL AVE.**  
**FORT CARSON, CO 80913-4145**

**COMMAND POLICY**  
**G6--01**

AFYB-CG

**AUG 05 2009**

MEMORANDUM FOR SEE DISTRIBUTION

Subject: 4<sup>th</sup> Infantry Division (4ID), G6 Information Assurance Policy

1. References.

- a. AR 25-2, Information Assurance (IA), dated 24 October 2007.
- b. DoD Directive 8500.1E, Information Assurance (IA), dated 24 October 2002.
- c. DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), dated 28 Nov 2007.
- d. FORSCOM G3 Memorandum "Appointment of Unit Information Assurance Manager (IAM) in Support of the FORSCOM Information Assurance Training and Certification Program," dated 29 October 2008.
- e. 4ID Information Assurance Standing Operating Procedure (IASOP), Draft.
- f. FORSCOM IA GUIDE, dated 03 April 2009

2. Purpose. Information Assurance begins at the lowest level and is mission critical in today's operating environment. This policy highlights critical components of the 4ID Information Assurance Program leaving specific and technical details to be covered in the 4ID IASOP (ref. e).

3. Applicability. This policy is applicable to all United States military personnel and civilians serving with, employed by, or accompanying the Armed Forces of the United States, while assigned to the 4ID or while present in the 4ID AOR who plan, deploy, configure, operate, and maintain Automated Information Systems (AIS) directly or indirectly attached to 4ID Networks.

4. Policy. This policy letter provides direction for implementation of IA requirements as defined in Public Law, DOD, and Army directives, policies, and regulations. The policies listed below are highlights from the 4ID IASOP but are not an inclusive list of the IA requirements for units.

- a. As outlined in a FORSCOM Memorandum (ref. d), each brigade must designate an IAM (O3/53A or CW2/254A). The IAM will ensure all members of the units IA team (see ref. e) are

designated on orders, registered on Army Training Certification and Tracking System (ATCTS), and current on required training.

b. All personnel requiring access to an AIS associated with 4ID must review and sign an Acceptable Use Policy prior to gaining access to a system. In addition, individual training will be completed annually and tracked at the unit level as defined in the 4ID IASOP (ref. e).

c. IAW AR 25-2 (ref. a) and DIACAP (ref. c) BDE and above units must accredit their SIPR network for home station and deployment. NIPR Information Systems will be accredited for deployment only.

(1) The 4ID IASOP provides key information about different paths for obtaining accreditation along with example accreditation packets (ref. e).

(2) Units must insure that all Minimum IA requirements are met IAW paragraph 4-5 of AR 25-2 and the 4ID IASOP (see ref. e for detailed requirements).

(3) A Continuity of Operations Plan (COOP) is required as part of the accreditation process. Units must identify Mission Essential Functions (MEFs), a COOP site, back-up procedures for sensitive/non-sensitive data, and a semi-annual test plan of the COOP (see ref. e for definitions and details).

d. All hardware/software approved for use on 4ID Information Systems (IS) will be maintained in the 4ID IASOP and any additions or deletions must be approved by the Change Control Board (CCB) that meets monthly in the G6 section (see ref. e). After approval by 4ID CCB, 4ID G6 will forward all additions to the FORSCOM Tactical Data System (TDS) technical POC for submission to the FORSCOM CCB for update of their approved HW/SW lists.

e. All 4ID IS Security Incidents involving information security breaches (as defined in 4ID IASOP ref. e) and spillages are reported from the unit IMO through the unit IA team up to the Division IAM within two hours of occurrence.

(1) Security Incidents: Division IAM reports to FCCO DOIM who then reports to RCERT. Security Incidents include any abnormal or suspicious activity that cannot be dismissed as normal operation of the system. Upon reporting, the IMO shall "Isolate" the system while leaving it powered up. Isolation includes unplugging the network connection, restricting direct physical access, and blocking the IP at security routers or firewalls both inbound and outbound.

(2) Spillage Incidents: Division IAM contacts and 4ID Security Manager (G2) and FORSCOM IAPM/IAM. Spillage occurs when classified information is inadvertently placed or transferred to an IS that has a lower classification level. Reporting unit must establish the number of systems affected, media and networks affected, classification, manner of spillage, and originator of information. Affected systems will be isolated by disconnecting the network cable but remain powered up. Division IAM ensures immediate notification is made to the recipients and the originator of the information through VoSIP.

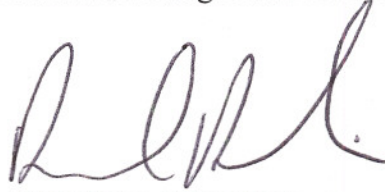


AFYB-CG

Subject: 4<sup>th</sup> Infantry Division (4ID), G6 Information Assurance Policy

f. 4ID SIPR Policies: Units must ensure their Protective Distribution System (PDS) are inspected (IAW 4ID IASOP) prior to each duty day for any signs of intrusion or tampering in all ZONE 1 areas (see ref. e). Inspection logs will be maintained for one year.

5. POC for this policy is the 4ID Information Assurance Manager at DSN 503-0616 or DSN 503-0604.

A handwritten signature in dark ink, appearing to read 'D. Perkins', is positioned above the printed name.

DAVID G. PERKINS  
MG, USA  
Commanding

DISTRIBUTION

A